合同编号：

陕西省公安厅交通管理总队
业务应用系统等保测评及密码测评项目

（第二标段：商用密码应用安全性评估）

技术服务合同

同意，请财务部办理。11/11

甲　方　：　陕西省公安厅交通管理总队

同意，呈领导审签。11/11

乙　方　：　智巡密码（上海）检测技术有限公司　张春光 11/13

签订时间：　2025 年 11 月 17 日

呈张处长审签。杨志昭 13/11

该合同已按方审计意见修改完成。

杨志昭 2025.11.13

依据《中华人民共和国民法典》及相关法律法规，经双方友好协商，就甲方委托乙方提供业务应用系统等保测评及密码测评项目密码应用安全性评估技术服务相关事宜达成一致，特订立本合同。

第一条 技术服务的内容、方式和要求

1. 技术服务内容：根据甲方要求，乙方负责对 业务应用系统等保测评及密码测评项目开展密码应用安全性评估提供技术服务。

乙方依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）标准，参照《商用密码检测机构管理办法》、《商用密码应用安全性评估管理办法》、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》等要求，制定测评实施方案，采取合理、有效、安全、科学的策略开展测评，并确保在测评过程中不影响被查系统的正常运行。

2. 技术服务方式：乙方到被测评系统所在地开展现场测评工作。

3. 技术服务要求：乙方完成系统测评后，应按要求认真汇总分析工作情况，每个检查系统出具测评报告，及时提交给甲方。

第二条 技术服务的期限及其他执行条款

1. 技术服务期限为：3 日历天完成测评准备活动，3 日历天完成方案编制活动，12 日历天完成现场测评活动，12 日历天完成分析与报告编制活动，5 日历天完成售后服务及培训、备案。

2. 验收及报告：《商用密码应用安全性评估量化评估规则（2023 年）》《信息系统密码应用高风险判定指引》《商用密码应用安全性

评估FAQ（第三版）》《商用密码应用安全性评估报告模板（2023版）》

《密码应用安全性评估结果备案流程（2023 版）》乙方提供的服务符合国家、地方及相关政府管理部门和行业与本项目有关的各项服务标准、规范、规章要求，并满足采购人实际需求，标准、规范等不一致的，以要求高的为准。

乙方遵循中华人民共和国及地方的有关法律规范，严格按照符合国家标准和行业标准及合同要求，符合招标文件、投标文件、澄清文件和中标通知书的要求等及采购人要求实施项目服务，在陕西省公安厅交通警察总队指定地点，按照“3日历天完成测评准备活动，3日历天完成方案编制活动，12日历天完成现场测评活动，12日历天完成分析与报告编制活动，5日历天完成售后服务及培训、备案”时间要求对部署在本地机房、省政务云、三秦警务云等环境的18个信息系统（三级）提供商用密码应用安全性评估，并保证交付的成果文件已参照已有的相关规划，并符合本项目服务要求。

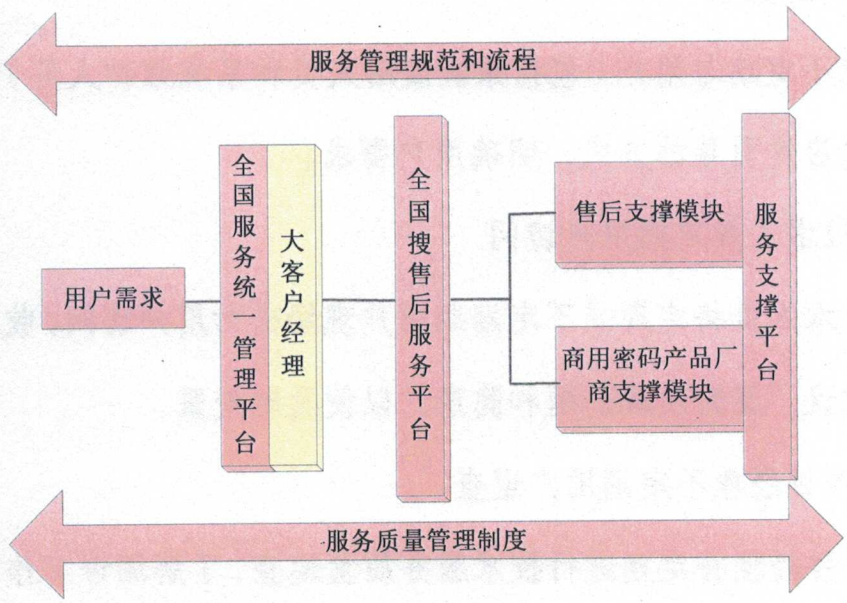
乙方按照项目要求以及合同约定时间和方式完成相应的服务支持和项目交付，项目进入验收阶段。双方履约至验收条件具备时，采购人应及时根据合同的规定进行项目验收。以书面形式向用户方提交《商用密码应用安全性评估报告》及相关材料。

用户方在收到服务提供方提交的密码应用安全性评估资料（服务周期内的服务过程文档和服务总结报告等）后，采购人进行项目验收并签署验收报告等，在服务期限结束前完成验收，验收小组成员签订验收报告，本项目正式结束。

3. 交付内容及售后服务

交付内容为乙方在完成项目约定的技术服务内容后，向采购人提出书面的验收申请，采购人按照项目约定进行验收。测评机构应完成项目验收资料的准备，包括但不限于出具经权威机构认可的《商用密码应用安全性评估报告》，确保报告内容的准确性和权威性。按照省级项目验收管理办法执行。由建设单位组成验收小组进行验收，双方根据最终验收情况，编写验收报告。

售后服务：为了更好的为用户提供服务，智巡密码（上海）检测技术有限公司提供“321”服务体系，“3”指三个服务平台，包括全国服务统一管理平台、全国服务实施平台以及服务支撑平台。“2”指两类制度，一类是服务管理规范和流程，另一类是服务质量管理制度。“1”指大客户经理，具体参见下图所示：



服务体系

全国服务统一管理平台主要负责服务制度和规范的制定、人员培

训、设备维修管理、备品备件规划、服务质量监测、全国售后服务电话接听和受理等。

乙方承诺在本次密码评测项目中按照以下方式建立售后服务体系：

(一)建立用户支持计划

为了更好地为用户提供技术支持服务，我方将建立用户支持计划。首先建立用户档案，明确用户基本信息，包括：用户单位、地址、联系方式、主要服务内容范围等；同时建立用户故障跟踪机制，详细记录用户本次计划测评的三级系统的故障处置情况，按照重大故障、一般故障、重要保障、一般保障四个不同级别接收、处置、反馈和记录用户故障，同时围绕用户档案，有计划地进行用户支持服务，主要包括：

（1）电话交流

定期或不定期与用户（包括系统使用人员和系统维护人员）进行交流，采用启发引导的方式，明确用户需求。

（2）技术人员定期用户访问

我方技术人员将定期或不定期到用户现场进行用户访问，收集用户意见和建议，及时发现问题和隐患，以便及时处置。

（3）项目经理不定期用户巡查

我方项目经理将定期进行技术服务质量巡查，了解测评工作完成后，在售后服务程中的问题，并针对发现问题及时整改。

（4）设立专业技术支持小组

当用户遇到各类紧急故障时，我方除安排专职技术人员按照流程进行故障解决外，还将组织一批经验丰富、技术过硬的人员组成专业技术支持小组，为用户和我方派驻的技术工程师提供全面支撑。

(二) 售后管理咨询

由于项目测评过程中需要统筹协调的方面很多，我方将提供经验丰富的项目售后服务人员，提供专业化的售后服务。

(三)周期性售后技术支持总结

乙方将周期性地在售后服务过程中进行技术总结，为用户科学分析现有密码体系=使用情况，涉及内容包括在过去工作过程中所出现问题的总结，可能存在的技术瓶颈分析，并对今后密码体系统运行提出合理建议。

(四)资料传送/专题讨论

定期或不定期给用户发送有关产品和技术的最新资料，并邀请用户参加乙方举办的专项技术研讨会，介绍有关技术的最新进展。

(五)合同约定外的有偿服务

针对维护合同之外的服务内容，乙方提供免费售后技术服务。

（1）遵循法律法规：承诺在评估工作的全过程中，严格遵守国家及地方颁布的各项法律法规、政策文件及行业标准。这包括但不限于评估行业的专门法规、数据保护法规、环境影响评估条例等，确保评估活动的合法性、合规性和公正性。

（2）执行标准规范：严格依据当前公认的评估标准、规范及最佳实践进行操作。这些标准可能涉及数字资产、部署环境、安全风险

等多个维度，确保评估结果的客观性、准确性和可比性。

（3）保证项目质量：深知项目质量的重要性，因此将采取一系列质量控制措施，包括但不限于组建专业团队、制定详细工作计划、实施严格的内部审核和外部复核等，以确保评估工作的高质量完成。同时，我们还将注重数据的真实性和可靠性，确保评估报告的科学性和权威性。

（4）按时交付成果：承诺在合同约定的时间框架内，高效有序地完成评估工作，并按时向客户提供评估报告及其他相关成果。我们将通过科学的时间管理和资源配置，确保项目进度的可控性和可预测性。

（5）持续沟通与反馈：在项目执行过程中，与客户保持密切沟通，及时汇报项目进展，听取客户意见和建议，并根据客户需求进行相应调整。同时，我们也将积极接受监管部门的监督和指导，确保评估工作的透明度和公信力。

（6）保密与隐私保护：评估过程中可能涉及客户的敏感信息和商业机密，因此将严格遵守保密协议和隐私保护政策，确保客户信息的安全性和保密性。

4. 乙方关于执行“安全技术测评”、“安全管理测评”、“密评工作原则”

（一）“安全技术测评”

乙方提供的密评服务主要内容涵盖密码应用通用要求测评、密码技术应用测评：

（1）密码应用通用要求测评：包括密码算法、密码技术、密码产品、密码服务等四个维度的通用测评。

1）密码算法合规性：主要针对信息系统中使用的密码产品、密码服务以及密码算法实现的合规性进行测评。

2）密码技术合规性：主要针对信息系统中的密码产品、密码服务以及密码技术实现的合规性进行测评。

3）密码产品合规性：主要针对信息系统中的密码产品的合规性进行测评。

4）密码服务合规性：主要针对信息系统中的密码服务的合规性进行测评。

（2）密码技术应用测评：包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个层面的安全测评。

1）物理和环境安全：主要针对“身份鉴别”、“电子门禁记录数据存储完整性”、“视频监控记录数据存储完整性”等物理和环境安全方面采取的密码保障措施进行各项测评。

2）网络和通信安全：主要针对“身份鉴别”、“通信数据完整性”、“通信过程中重要数据的机密性”、“网络边界访问控制信息的完整性”、“安全接入认证”等网络和通信安全方面采取的密码保障措施进行各项测评

3）设备和计算安全：主要针对“身份鉴别”、“远程管理通道安全”、“系统资源访问控制信息完整性”、“重要信息资源安全标记完整性”、“日志记录完整性”、“重要可执行程序完整性、重要

可执行程序来源真实性”等设备和计算安全方面采取的密码保障措施进行各项测评。

4）应用和数据安全：主要针对“身份鉴别”、“访问控制信息完整性”、“重要信息资源安全标记完整性”、“重要数据传输机密性”、“重要数据存储机密性”、“重要数据传输完整性”、“重要数据存储完整性”、“不可否认性”等应用和数据安全方面采取的密码保障措施进行各项测评。

（二）“安全管理测评”

乙方提供的密评服务主要内容涵盖密码应用安全管理测评、密钥管理安全性测评：

（1）密码应用管理要求测评：对影响商用密码防护效能的管理制度与措施进行分析与评估。包括分为管理制度、人员管理、建设运行和应急处置等四个层面的安全测评。

1）管理制度：针对“具备密码应用安全管理制度”、“密钥管理规则”、“建立操作规程”、“定期修订安全管理制度”、“明确管理制度发布流程”、“制度执行过程记录留存”等制度方面采取的管理措施进行各项测评。

2）人员管理：针对“了解并遵守密码相关法律法规和密码管理制度”、“建立密码应用岗位责任制度”、“建立上岗人员培训制度”、“定期进行安全岗位人员考核”、“建立关键岗位人员保密制度和调离制度”等人员方面采取的管理措施进行各项测评。

3）建设运行：针对“制定密码应用方案”、“制定密钥安全管

理策略”、“制定实施方案”、“投入运行前进行密码应用安全性评估”、“定期开展密码应用安全性评估及攻防对抗演习”等实施方面采取的管理措施进行各项测评。

4）应急处置：针对“应急预案”、“事件处置”、“向有关主管部门上报处置情况”等应急方面采取的管理措施进行各项测评。

（2）密钥管理安全性测评：包括密钥管理（密钥产生、分发、存储、使用、更新、归档、撤销、备份、恢复与销毁等）的安全测评。对密钥的产生、分发、储存、使用、更新、归档、撤销、备份、恢复和销毁等环节进行管理和策略制定的全过程进行测评。

（三）“密评工作原则”

乙方遵循以下若干原则，是测评结论真实、准确、可信的基础，也是密码测评组在独立实施测评时，在相似的情况下得出相似结论的前提。

测评技术原则

为确保在独立实施评估时，在相似的情况下得出相似结论，保障密码测评结论的真实、准确、可信等。本项目的商用密码应用安全性评估实施方案设计与具体实施满足遵循“客观公正、经济性和可重用性、可重复性和可再现性、结果完善性”原则，具体细节内容如下：

（1）客观公正原则：基于法律法规及政策文件要求、国家标准和行业技术规范以及项目需求和技术服务规格等内容中明确定义的评估方式和解释，项目实施测评工作组的测评工程师在最小主观判断情形下按照双方（被测评单位和第三方测评机构）共同认可的测评方

案，来保证密码测评实施过程中技术人员在最小主观判断情形下实施密码测评活动。

（2）经济性和可重用性原则：当待评估对象已有评估结果（主要包括：商用密码应用安全性评估结果或密码应用方案评估结果等）的前提情况下，开展实际评估工作时存在适用于待评估对象的所有重用结果都适用（包括但不限于全部或部分情况已有评估结果等场景）且可直接重用已有评估结果，来保证能够客观反映目前待评估对象的安全状态。

（3）可重复性和可再现性原则：可重复性体现出在不同评估者评估结果的一致性，可再现性聚焦于同一评估者评估结果的一致性。不同的评估机构、不同的技术人员依照同样的要求，使用同样的评估方法对每个评估实施过程的重复执行应得到同样的结果，来保证评估结果一致性。

（4）结果完善性原则：基于正确理解《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》各个要求项内容的基础之上，按照认可的测评方案和正确的评估方法实施密码测评活动，待评估对象检测所有评估过程以及产生的评估结果严格遵守且客观完全满足规范要求，来保证能够客观反映系统的运行状态。

测评实施原则

本次商用密码应用安全性评估实施活动与具体实施服务规格应满足以下原则：

（1）保密性原则：在测评过程中，需严格遵循保密原则，采购

人与供应商签订保密协议和非侵害性协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害用户利益。在测评过程中，切实加强对人员、技术等方面的组织管理，确保在项目实施过程中涉及的所有信息，不会泄露给第三方单位或个人，不擅自利用这些信息。

（2）规范性原则：商用密码安全性评估服务的实施由专业的评估服务人员依照规范的操作流程进行，对操作过程和结果要有相的记录，并提供完整的服务报告。根据项目实施的需要及要求，在人员、质量和时间进度等方面进行严格管控，在保证测试质量的前提下，按计划进度执行。安全测评工具、方法和过程要在双方认可的范围之内合法进行。

（3）最小影响原则：在项目实施的过程中，严格遵守工作场所的相关管理规定及安全、保密、机房准入等规章制度，确保安全生产、安全作业。任何对网络的操作均要有采购人陪同，并在许可下进行。在项目实施的过程中，充分考虑到相关活动对系统正常运行的不利影响，采取必要的措施将相关风险降到最低，测评过程尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响(包括系统性能明显下降、网络阻塞、服务中断等)，如无法避免，则应预先做出说明并经采购人同意后实施，不能对正常运行的系统和网络构成破坏。

（4）完整性原则：在测评过程中，严格遵循测评方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够

的证据，发现其存在的密码应用安全性问题。测评内容覆盖密码测评方案描述的测评对象、测评指标、测评检查点、单元测评实施内容等，获取分析与报告编制活动所需且足够的证据和资料。同时确保整体测评数据、过程记录以及证据和资料采集的完整性。

（5）质量保障原则：在整体测评服务过程特别重视项目质量管理，强调合规性、全面性、客观性、持续改进与保密性。严格遵守国家法律法规，全面评估商用密码技术应用，保持评估过程客观公正，持续优化评估流程和方法，并严格保守重要数据信息，以确保密评工作的权威性、准确性和安全性。项目实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

第三条 技术服务费用及结算方式

1. 甲方应向乙方支付的技术服务费用总额为：147.6 万元（大写：壹佰肆拾柒万陆仟元整 ）。

2. 支付方式：

签订合同后，达到付款条件起 30 日内，支付合同总金额的 30.00%。

初验合格后，达到付款条件起 30 日内，支付合同总金额的 40.00%。

终验合格后，达到付款条件起 30 日内，支付合同总金额的 30.00%。

3. 乙方应满足付款节点要求后的 7 个工作日内向甲方开具正规等额发票，甲方需提供开票信息。

第四条 双方权利义务

1. 甲方权利义务

（1）甲方有权对乙方项目的执行情况、项目目标达成情况和经费使

用情况进行监督检查；

（2）甲方有权要求乙方报告项目密码应用安全性评估工作情况，并提供相关的证明材料；

（3）甲方对乙方开展技术服务工作给予必要的协助，配合乙方提出的合理工作需要；

（4）　甲方应按合同约定及时、足额向乙方支付技术服务费用。

2. 乙方权利义务

（1）乙方负责项目的组织及执行，确保按照相关要求落实项目密码应用安全性评估工作；

（2）乙方负责如实、客观地向甲方报送项目进展情况、项目目标达成情况；

（3）乙方应按时提交测评报告。

第五条 保密义务

1. 与本合同相关的任何文字、图形、图像以及方案、技术信息、知识产权、被测系统的相关信息等，均属于本合同相关方的技术秘密或商业秘密，双方须严格遵守，未经一方同意，任何一方不得向第三方披露对方的上述信息，但法律法规另有强制性规定的除外（在此情形下，信息披露方应在法律法规允许的前提下尽早将相关情形通知另一方）。

2. 本条为持续性条款，自本合同生效之日起持续有效，不因本合同的变更、解除、终止而终止。

第六条 不可抗力

1. 因受不可抗力影响而不能履行或不能完全履行本合同的一方可以部分或全部免除其责任。

2. 遇有不可抗力的一方，应立即将事件情况以书面形式通知对方，并在15日内提供事件详情以及合同不能履行或部分不能履行或需要延期履行的理由的有效证明文件。根据事件对履行合同的影响程度，由双方协商决定是否解除合同、部分免除责任或延期履行。

3. 如因不可抗力需要变更本合同部分条款的，双方可通过协商达成进一步履行协议的协议。

第七条 违约及争议解决

1.任何一方违反本合同约定，守约方有权要求违约方在指定时间内纠正其违约行为。

2.就本合同的解释、效力或履行所产生的争议，甲乙双方应通过友好协商解决。协商不成的，任何一方可向合同签订地人民法院提起诉讼。

第八条 其他

1. 本协议任何变更、修改须经甲乙双方协商一致，并签署书面补充协议，作为本合同的一部分，与本合同具有同等法律效力。

2. 本合同经双方法定代表人或授权代表签署并加盖单位公章（或合同专用章）后生效，至双方权利义务履行完毕之日终止。

3. 本合同一式陆份，甲方叁份，乙方叁份，具有同等法律效力。

以下无正文

甲方（章）：

陕西省公安厅交通管理总队

法定代表人或授权代表：

通信地址：西安市长安南路 123 号

联系人：

联系电话：029-87680118

日期：2025.11.17

乙方（章）：

智巡密码（上海）检测技术有限公司

法定代表人或授权代表：

通信地址：上海市松江区沐川路 58 弄 1 号 5 楼

联系人：秦琼

联系电话：13891800525

日期：2025.11.17

开户银行：交通银行上海泗泾支行

账号：3100 6920 2018 8100 44439